NOTPETYA: WHY WOULD RUSSIA TARGET KASPERSKY AV?

With the backing of a bunch of security companies, both the US and Ukraine are getting closer to formally blaming Russia for the NotPetya attack last week on the same hackers that brought down the power grid in 2015.

But there are skeptics. Rob Graham suggests this analysis all suffers from survivorship bias. And Jonathan Nichols argues the attack was so easy pretty low level hackers could have pulled it off.

Nichols also raises a point that has been puzzling me. The attack does extra damage if it detects the Kaspersky Antivirus.

> Much has been made about the fact that the NotPetya virus appears to have been designed as a wiper, and not as a genuine piece of ransomware. The virus also checks for avp.exe (Kaspersky Antivirus) and then wipes the bootsector of any device with the file present.
>
> [snip]
>
> Further, the specific targeting of Kaspersky Antivirus harkens back to the vindictive nature of low level cyber criminals, such as those which famously write hate messages to Kaspersky and Brian Krebs regularly.

There may be a good reason to do this (such as, if Kaspersky dominates the AV market in Ukraine, it would provide an additional way to target Ukraine specifically, though that would seem to also implicate Russian companies, like Rosneft, that were hit by NotPetya as well). But absent such a reason, why would Russia selectively do more damage to victims running Kaspersky, especially at a moment with the US is so

aggressively trying to taint Kaspersky as a Russian front?

As a reminder, back in January when Shadow Brokers claimed to be disappearing forever, they called out Kaspersky specifically in a dump of dated Windows files (SB trolled Kaspersky even more on Twitter, though deleted all those old tweets last week).

> Before go, TheShadowBrokers dropped Equation Group Windows Warez onto system with Kaspersky security product. 58 files popped Kaspersky alert for equationdrug.generic and equationdrug.k TheShadowBrokers is giving you popped files and including corresponding LP files.

So not just cybercriminals with a grudge against Kaspersky for cooperating with western law enforcement, but the source of some of the exploits used in this attack, has targeted Kaspersky in the past.

I don't know the answer. But it's one counterargument to the rush to blame Russia that, in my opinion, needs some answers.